MAZEBOLT

STATE OF DDOS DEFENSES SURVEY

More Spend. More Attacks. Less Confidence.

What 300 CISOs and security directors told us about DDoS readiness.

63% say their DDoS protection is mostly automated **but** **99%** still rely on manual tests to validate there are no vulnerabilities

72% are confident defenses stop attacks automatically **but** **42%** suffered DDoS damage in the past 12 months

99% test using maintenance windows **but** **<200** attack vectors are tested, out of thousands

85% increased DDoS budget **but** **5%** are fully confident it's working as intended

86% test DDoS defenses just once a year or less **but** **100%** experienced at least one damaging attack in the past 12 months

97% see value in continuous, nondisruptive DDoS testing **but only** **9%** actually understand it in depth

DDoS Testing is Disruptive

Maintenance windows are disruptive. Traditional testing is scheduled in off-peak hours to minimize disruption.

This approach:

- Restricts testing **duration** to narrow time slots
- Limits testing coverage to a **fraction** of the attack surface
- Produces results that quickly **lose relevance**

Continuous, Nondisruptive DDoS Testing Matters

Ongoing DDoS attack simulation on known and AI-generated attack vectors ensures vulnerabilities are identified before an attack occurs.



To learn more, download the full report.

GET REPORT →

MAZEBOLT